Trusted Agent-Mediated E-Commerce Transaction Services via Digital Certificate Management *

Yuh-Jong Hu (jong@cherry.cs.nccu.edu.tw)
Emerging Network Technology (ENT) Lab., Department of Computer Science, National Chengchi University, Taipei, Taiwan

Abstract.
Agent-mediated e-commerce (AMEC) transaction services will be a paradigm shift from the existing client-server e-commerce model. In order to fulfill the leverage of AMEC intermediary services with secure and trusted service capabilities, we propose an agent-oriented public key infrastructure (PKI) operating with a variety of digital certificates. Under this agent-oriented PKI, several trusted AMEC transaction service models will be demonstrated using human and agent certificates showing, delegation, and verification protocols. We establish human/agent authentication, authorization, delegation, access control, and trusted relationships before these trusted AMEC intermediary services can be realized. This paper shows that a trusted AMEC system can be implemented in the FIPA compliant multi-agent system.

Keywords: agent-oriented pki, agent-mediated e-commerce (AMEC), agent trust and delegation, digital certificate, FIPA standards

1. Introduction

The proliferation of electronic commerce (e-commerce) did not eliminate mediator services on the Internet. Electronic mediators, i.e., software agents, will play very important roles in the e-commerce mediation services (Bailey and Bakos, 1997)(Sarkar et al., 1995). The economic implications of agent technology and e-commerce are very promising in the near future (Vulkan, 1999). Agents as mediators in e-commerce services are likely to be roles that possibly include aggregating and filtering information, providing trust and secure relationships to ensure the integrity of the market, negotiating e-commerce transaction service criteria, and matching consumers and suppliers, etc (Moukas et al., 2000).

Unfortunately, it is still unclear from the existing published agent research literature what the important core research issues that need

* This paper was accepted by Electronic Commerce Research (http://www.kluweronline.com/issn/1389-5753/contents) and will be published on Volume 3 Issues 3-4, 2003. This research was supported by Taiwan National Science Council (NSC) under grants No. NSC 89-2213-E-004-002 and NSC 90-2213-E-004-008.

to be addressed in agent-mediated e-commerce (AMEC) (Nwana et al., 1998)(Sierra, 1999). Several issues and challenges have emerged in AMEC research in the past few years. Among them, building a trusted and secure agent service infrastructure for multi-agent mediators to provide a trustworthy service environment is most important. If agent trust and security issues are not solved, it is nearly impossible to apply agent technology in a legal manner for e-commerce transaction services (Heckman and Wobbrock, 2000).

An agent is a software program embedded with *autonomy, proactive, reactive,* and *social* features (Jennings et al., 1998). To be an electronic mediator, the agent must fulfill these service characteristics to leverage e-commerce transaction mediation services.

Agent-based e-commerce transaction services is a paradigm shift from the existing client-server transaction model. In this new paradigm, people use a browser and web server as interface windows to initiate multi-agent transaction services. In this paper, we will show how a multi-agent can use different digital certificates to achieve trusted transaction mediation services under an agent-oriented public key infrastructure (PKI). Digital certificates are classified into several categories including identity certificate, attribute certificate, authorization certificate, and rule certificate. The identity certificate is vouched by well-known certification authority (CA) to ensure principal authentication. The attribute certificate is issued by an attribute authority (TA) to indicate the principal's attribute status. The authorization certificate is initiated by a resource provider to provide flexible delegation among agents. The rule certificate is a new certificate category that we propose to express resource access control policies. Several trusted AMEC models will be explicitly operated using our digital certificate verification protocols.

In summary, the primary objectives of this research includes the following issues:

- Resolve agent trust, delegation, authentication, and authorization relationships before trusted AMEC transaction services can be achieved.

- Design a digital certificate classification scheme to ensure agent authentication, authorization, and delegation services criteria for trusted AMEC.

- Implement trusted AMEC transaction service models using certificates showing, delegation, and verification protocols.

2. Research Background

2.1. Digital certificates

A digital certificate (or digital credential) concept was first proposed by Kohnfelder (Kohnfelder, 1978). The digital certificate is defined as a digital statement signed by an *issuer* verifying some *attributes (or profiles)* of a *subject* for a valid period using the issuer's private key. The X.509 identity certificate was proposed first for human identification in the client-server e-commerce transaction service. The attribute certificate was proposed recently to support the identity certificate in relation to the principal's authorization (Park and Sandhu, 2000). In (Ellison, 2001), a delegated authorization certificate SPKI/SDSI was proposed using the issuer and subject's public keys with authorization expression within the 5-tuple format.

The digital certificate is more robust and flexible than password or other conventional access control mechanisms for principal authentication, authorization, and delegation control on the open Internet environment. It is not a new idea using certificates for principal authentication and authorization on the World-Wide Web (Winslett et al., 1997). Unfortunately, most existing digital certificates were proposed only for the client-server transaction service model or pure distributed system environment (Aura, 1999)(Blaze et al., 1999). They are therefore not suitable for the multi-agent AMEC transaction service environment.

2.2. Agent trust issues

Why are we so interested in solving the agent trust issue in the AMEC service environment? If we can not solve the agent trust problem, people are not going to adopt agents as electronic mediators. If we can not provide a reliable and trustworthy delegation mechanism, people will be hesitant to proceed with any e-commerce transaction via agent mediators.

There were some attempts at solving multi-agent system trust and security issues using conventional security techniques, but these methods were not based on certification theory with building agent-oriented PKI in mind (He et al., 1998)(Wong and Sycara, 1999). We doubt the feasibility of integrating these approaches with emerging multi-agent framework standards, such as FIPA.

There are many facets of trust in AMEC services. Trust can be defined as reputation mechanisms that rely on a collaborative rating and personalized evaluation (Zacharia and Maes, 2000). From the delegation analysis viewpoint, people regard trust as a background status for

delegation. The trust loop is therefore not equal to the delegation loop. For example, we might trust something (or someone) without granting our authority under some prohibitive conditions. Therefore, trust is a *necessary* but not *sufficient* condition for delegation (Castelfranchi and Falcone, 2000).

We defined trust as an authentication, authorization, and delegation verification problem involving digital certificates with showing and verification protocols. This low level of trust must be satisfied before any high level organization or psychological trust can be achieved. This idea can be explicitly shown in the resources or services access control problem on the Internet. Because it is almost impossible for all principals to be registered members of the resource provider in a distributed services environment, digital certificate delegation mechanisms can provide the capacity to deal with trust establishment with a stranger (Herzberg et al., 2000).

In this paper we explicitly show the agent delegation in the Lampson's delegation logic with digital certificates as associated verification facts and rules in the policy assertion engine (PAE) (Lampson et al., 1992). Agent trust can be verified in terms of its authentication, authorization, and access control criteria using logic-based inference rules. More specifically, evaluation and demonstration of this concept will be shown in a variety of AMEC transaction service models, such as customer to business (C2B), customer to customer (C2C), business to business (B2B), and peer to peer (P2P).

3. Digital certificates classification

3.1. Identity certificate

The identity certificate ($ID - Cert$) is a digital assertion that shows the binding of a subject's unique identification with his public key certified by the certification authority (CA) (Gerck, 2000). A principal[1] p's identity certificate $ID_{CA \mapsto p} - Cert$ is defined as:

$$ID_{CA \mapsto p} - Cert = (Id_p, Pu_p, V, Option, Sig_{CA})$$

where:
Id_p: principal p's distinguished identity.
Pu_p: principal p's public key.
V: validation period for identity certificate.

[1] Principal p might be human(h) or agent(a) in this study

$Option$: optional information.
Sig_{CA}: certificate signature signed by CA's private key.

3.2. Attribute certificate

The attribute certificate ($AT-Cert$) is a digital statement that indicates the binding of a subject's identification with his attributes information with the exception of his public key. This $AT-Cert$ is issued and authorized by the attribute authority (TA) (Farrell and Housley, 2001). The analogy to real life is that we usually have only one identity certificate but we might have multiple attribute certificates, such as credit cards, driver licenses, ATM cards, etc. A principal p's attribute certificate $AT_{TA\mapsto p}-Cert$ is defined as:

$$AT_{TA\mapsto p}-Cert=(Id_p, Ar_p, V, Option, Sig_{TA})$$

where:
Id_p: principal p's distinguished identity.
Ar_p: principal p's attribute information.
V: validation period for attribute certificate.
$Option$: optional information.
Sig_{TA}: certificate signature signed by TA's private key.

3.3. Authorization certificate

The authorization certificate ($AU-Cert$) is a digital credential that binds the issuer's authorization and subject's public keys with associated authorization information delegated from the authorization authority (AA).

The authorization certificate $AU-Cert$ for principal p delegates to principal q is similar to the SPKI/SDSI authorization certificate as shown in (Ellison, 2001):

$$AU_{p\mapsto q}-Cert=(Pu_p, Pu_q, A, D, V, Sig_p)$$

where:
Pu_p: a public key for the issuer of principal p to grant authorization.
Pu_q: a public key for the subject of principal q to receive authorization.
A: expression for authorization.
D: delegation bit with value 0 or 1.
V: validation period for authorization certificate.
Sig_p: certificate signature signed by p's private key.

3.4. Rule certificate

The $RU - Cert$ is certified by any rule authority (RA) who has the right to provide mediation services or to control the tangible or intangible resources (Johnston et al., 1998)(Winsborough et al., 1999). Rule certificate $RU_{RA \mapsto RS_i} - Cert$ with respect to the resource RS_i access authority in RA is defined as:

$$RU_{RA \mapsto RS_i} - Cert = (RS_i, Assertions, Sig_{RA})$$

where:
RS_i: access authority for resource(or service)[2] i.
$Assertions$: a set of rules in Conjunct Normal Form (CNF) to indicate the requirements of both identity and attribute certificates to unlock the resource access authority RS_i.
Sig_{RA}: certificate signature signed by RA's private key.

4. Agent-oriented PKI

An agent-oriented PKI with associated digital certificates are used to guarantee authentication, authorization, trust and delegation control criteria for both agent mediators and their owner.

This agent-oriented PKI is proposed to solve certificate management problems for both humans and agents. Human certificates are obtained via trust establishment in the physical world. Agent certificates are inherited, fused, and delegated from human certificates and used in cyberspace.

We propose that human and agent digital certificates are issued and managed by separate certificate administration sites. In general, the human identity and attribute certificates are issued and managed by well-known legal TTPs, i.e., HCA and HTA. Agent certificates are issued and managed by certificate management agents, such as ID_p-agent, AT_p-agent, AU_p-agent, and RU_p-agent in the agent platform (see *Figure 1*). An agent platform (AP) provides the physical infrastructure in which agents can be deployed. The AP consists of the machine(s), operating system, agent support software, FIPA agent management components and agents (FIPA01a, 2001a). On the client side, human and ordinary agent certificate management service agents

[2] In the AMEC service scenario, some of the agents might only provide pure mediation services while other agents are directly involved in physical tangible goods or intangible information resource access control. Thus, the rule certificate might correspond to either resource or service access control policies.

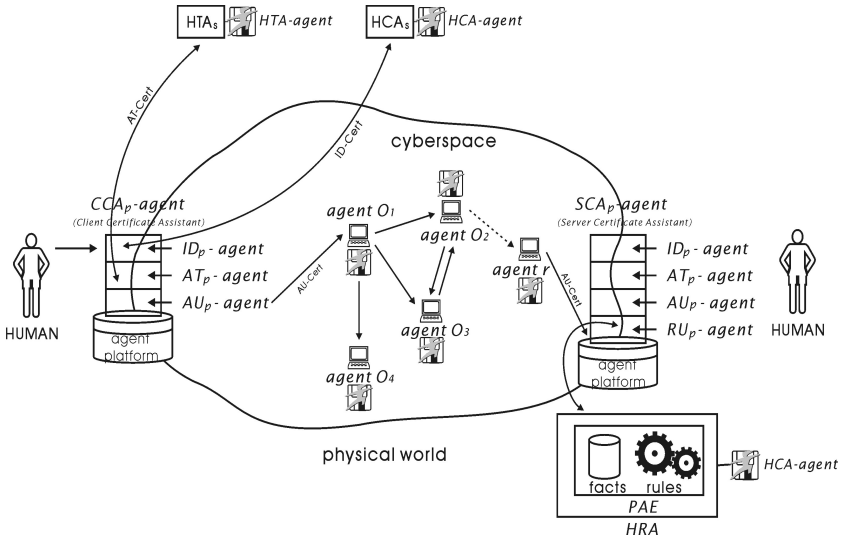

Figure 1. Agent-Oriented PKI to serve as trust establishment for human beings and agents via a group of agents to manage different kinds of digital certificates

$Cat_p - agent$, where $CAT \in (ID, AT, AU)$, are integrated as client certificate assistant $CCA_p - agent$ and on the server side, human and ordinary agent certificate management service agents $Cat_p - agent$, where $Cat \in (ID, AT, RU, AU)$, are integrated as server certificate assistant $SCA_p - agent$. These $CCA_p - agent$ and $SCA_p - agent$ concepts were also shown in Winslett's digital certificate studies (Winslett et al., 1997).

5. Agent trust vs. delegation and access control

5.1. Why delegate to agents

The reasons for human (or agent) delegator x to trust his delegatee agent y, then delegate his authority to the delegatee agent are possible because of the following reasons: the delegatee agent y is the right species for a particular service environment; delegator x might be in a mobile and wireless connection status and needs delegatee agent y to perform continuous follow-up services; delegatee agent y might have complete domain expert knowledge to achieve the goal; a group of delegatee agents concurrent services provide a highly efficient services, etc.

5.2. Trust vs. delegation

In a pure agent mediation service, the trustor agent x tries to achieve the goal G via the authority delegation to trustee agent y. Agent x must then have trust for its "competence" and "disposition" beliefs on agent y before this delegation is initiated. A "competence" belief indicates that agent y has the *capability* to complete the goal G whereas a "disposition" belief indicates that agent y has the *willingness* to finish the goal G. In our study, "competence" belief will be shown as an authorization certificate delegated from trustor agent x to trustee agent y. The "disposition" belief is shown as an acceptable service charge for agent y. Using either announcement in y's service registration or via x and y's negotiation protocols to derive an acceptable fees. The "disposition" belief will not be explicitly analyzed in this paper.

5.3. Trust vs. access control

Assuming that all of the identity and attribute certificate issuing authorities are TTPs and the resource access control agent has the complete rights to declare its acceptance policies to decide which CA and TAs are legal for issuing identity and attribute certificates. From the resource access control agent's viewpoint, the primary concern about agent trust vs. access control usually comes from the authorization certificates verification submitted by the resource request agents.

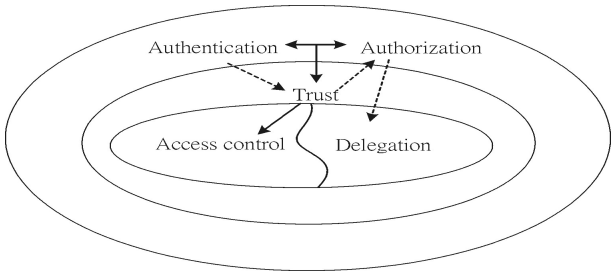

Figure 2. A progressive relationship for agent authentication, authorization, trust, and resources access control

The progressive relationships among the principal's authentication, authorization, trust, delegation, and resource access control can be shown in *Figure 2*. In *Figure 2*, the agent delegation path is shown as:

$$authentication \dashrightarrow trust \dashrightarrow authorization \dashrightarrow delegation$$

The resource access control path is shown as:

$$(authentication \leftrightarrow authorization) \rightarrow trust \rightarrow \text{access control}$$

5.4. Agent authority delegation

The human to agent authority delegation is based on the degree of human subjective trust level in the delegatee agent within an associated AMEC service domain. Of course, agents might apply the same principle to another agent in the chain-ruled delegation. First of all, delegator x initiates mutual authentication protocols with the delegatee agent y. Based on delegator x's subjective trust preferences on this particular AMEC service domain, delegator x will issue an authorization certificate to initiate an authority delegation.

Agent delegation mechanisms will be explicitly shown as in the Lampson et al. delegation logic (Abadi et al., 1993)(Lampson et al., 1992). In reality, delegation logic will be implemented as digital certificates using rules and facts within the policy assertion engine (PAE) in a secure agent management system.

- Complete authority delegation from principal A to principal B is denoted as either of the following:
  - Principal A says principal B(or $threshold(m, [B_1, \cdots, B_n])$) speaks for A on some authority under conditions $\sim$.
  - Principal A delegates some authority to principal B (or $threshold(m, [B_1, \cdots, B_n])$) under conditions $\sim$.
- Partial authority delegation as role is denoted as:
  - Principal A says principal B(or $threshold(m, [B_1, \cdots, B_n])$) speaks for A with role as $\sim$ on some authority under conditions $\sim$.

The above agent delegation logic with the associated digital certificates establishes the trust relationship for resource access control between a resource requester agent and a provider agent. The delegation logic inference processing is enforced by the PAE's *rules* and *facts*, where delegation logic expressions are **rules** and instances of $ID-Certs$, $AT-Certs$, and $AU-Certs$ are **facts**. This PAE will be initiated when the final resource requester agent r submits its request. An implementable and tractable delegation logic can be shown as a predicate clause similar to that in Li's study (Li et al., 1999):

```
H          If          F
```

where H is a head statement and F is a body formula. A predicate clause with an empty body is called a *fact*. A *query* takes the form: "F?",

where F is a body formula. A query is a request for an authorization certificate from $CCA_p - agent$ to $SCA_p - agent$. The answer to this query is quite similar to the rule inference resolving in Prolog or other Horn logic rule system by applying PAE facts and rules. Furthermore, the delegatee agent's service or resource request can be resolved using the PAE inference engine.

6. Digital Certificate Management

Human beings live in the real world and use digital certificates that are specifically designed for them, while agents live in cyberspace and use agent-oriented digital certificates for their trusted AMEC transaction services[3]. We explicitly separated human and agent identity certificates in order to differentiate between human and agent certificates showing, delegation, and verification protocols. We do believe that a human trust relationship must be established first to provide the original authority for agents to initiate their diverse delegation mechanism. For more detailed analysis see the following sections:

6.1. Trust establishment and authority granting

Human identity certificate $ID_{human} - Cert$ is issued by a global human CA (HCA), while the agent identity certificate $ID_{agent} - Cert$ is issued by a local CA (LCA) under each specific agent platform. When a single user initiates a group of mediator agents to perform a variety of e-commerce transaction services, it is impossible to require the tremendous number of agent identity certificates to be issued and managed using a well-known legal HCA. This is the reason why we separated the human and agent identity certificates issuing authority into two categories.

In the real world, a human might have several $AT_{HTA \mapsto h} - Cert$s issued by different well-known trusted HTAs. These attribute certificates along with the identity certificate provide a capacity for $CCA_{m_1} - agent$ to obtain its initial authorization certificate from $SCA_{m_2} - agent$ (see *Figure 3*). Conversely, the ordinary agent does not explicitly require an attribute certificate as a human being does because all of the authorities for the ordinary agent are delegated from $AU_{m_1} - agent$ embedded in $CCA_{m_1} - agent$.

[3] Digital certificates sometimes are designed for institutions instead of humans because the institution certificates are also re-issued under the authorization of a delegated person. We therefore only classified certificates into human and agents, two categories.

$RU_{RA \mapsto RS_i} - Certs$ are specified by $RU_{m_2} - agent$ embedded in $SCA_{m_2} - agent$ to declare the resource access control policies. Once $RU_{RA \mapsto RS_i} - Certs$ requirements are verified successfully for resources request, an $AU_{m_2 \mapsto m_1} - Cert$ will be issued from $AU_{m_2} - agent$ in $SCA_{m_2} - agent$ to $AU_{m_1} - agent$ in $CCA_{m_1} - agent$. The entire trust establishment scenario between $CCA_{m_1} - agent$ and $SCA_{m_2} - agent$ via digital certificate issuing, showing, and verification is shown in *Figure 3*.

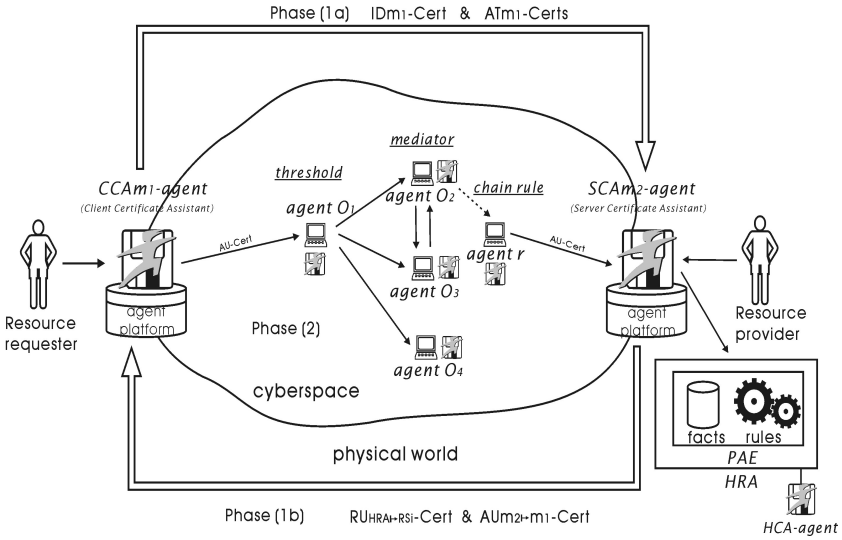

Figure 3. The trust establishment scenario for granting authority from $SCA_{m_2} - agent$ to $CCA_{m_1} - agent$ via human certificates issuing, showing, and verification (more detailed operations see section 6.2.1) are shown in phases (1a) and (1b). In phase (2), the agent certificates showing, delegation, and verification protocols (more detailed operations see section 6.2.2) are executed to achieve trusted AMEC transaction services.

6.2. Certificate Showing, Delegation, and Verification Protocols

The initial trust establishment for humans is based on the simple end to end authentication and authorization protocols between the $CCA_{m_1} - agent$ and $SCA_{m_2} - agent$. While the trust establishment among ordinary agents are more flexible with diverse delegation mechanisms, such as chain-ruled, threshold, and conditional delegation protocols.

6.2.1. *Human Certificate Showing, Delegation, and Verification Protocols*

1. Initial human certificate issuing and storing

   The client side user m_1 is assumed to be the resource requester and his certificate management task is controlled by the $CCA_{m_1} - agent$. This $CCA_{m_1} - agent$ is embedded into the $ID_{m_1} - agent$, $AT_{m_1} - agent$, and $AU_{m_1} - agent$ service capabilities. The server side user m_2 is a resource provider and his certificate management task is controlled by the $SCA_{m_2} - agent$. This SCA_{m_2}-agent is embedded into the $ID_{m_2} - agent$, $AT_{m_2} - agent$, $AU_{m_2} - agent$ and $RU_{m_2} - agent$ service capabilities (see *Figure 1*). In the AMEC P2P transaction service model, each user might simultaneously have a $CCA_{m1} - agent$ and $SCA_{m_2} - agent$ to provide associated services.

   Supposing that identity certificates $ID_{HCA \mapsto (m_1, m_2)} - Cert$ for human m_1 and m_2 were issued and stored in HCA by the HCA-agent and sent to $CCA_{m_1} - agent$ and $SCA_{m_2} - agent$ respectively. Several attribute certificates $AT_{HTA \mapsto m_1} - Cert$s and $AT_{HTA \mapsto m_2} - Cert$s were also issued and stored in the associated HTAs by the HTA-agent to declare m_1 and m_2's profile attributes. These $AT - Cert$s were issued after the $ID - Cert$s to ensure the binding feasibility. Furthermore, the $RU_{HRA \mapsto (RS_1, RS_2, \cdots, RS_n)} - Cert$s are also specified in the human rule authority (HRA) by the $RU_{m_2} - agent$.

2. The initial handshaking protocols between $CCA_{m_1} - agent$ and $SCA_{m_2} - agent$ query what the feasible set of $ID_{HTA \mapsto m_1} - Cert$ and $AT_{HTA \mapsto m_1} - Cert$s is to prepare to unlock the server resource access authority RS_i.

   - $CCA_{m_1} - agent$: Hello, I am m_1 user's agent (see my attached $ID_{HCA \mapsto m_1}$)[4] and ask you what kinds of $AT - Cert$s I have to prepare to unlock the resource access authority RS_i?
   - $SCA_{m_2} - agent$: Hello, I am m_2 user's agent (see my attached $ID_{HCA \mapsto m_2}$). Based on $RU_{HRA \mapsto RS_i} - Cert$s in my HRA, if you have the following certificates (in CNF) prepared[5]:

[4] The $SCA_{m_2} - agent$ might verify the validity of this $ID - Cert$ by checking the explicit unique distinguished name Id_{HCA} and Id_{m_1} with their public key. Similar authentication protocols can be applied to the other certificate categories.

[5] We did not require the $SCA_{m_2} - agent$ to provide similar attribute certificates for the $CCA_{m_1} - agent$ to verify. If this is not true, then automated negotiation protocols between the $CCA_{m_1} - agent$ and $SCA_{m_2} - agent$ are required (Winsborough et al., 1999).

$$(CAT_{issuer \mapsto subject} - Cert \vee \cdots \vee CAT_{issuer \mapsto subject} - Cert) \wedge \cdots \wedge$$

$$(CAT_{issuer \mapsto subject} - Cert \vee \cdots \vee CAT_{issuer \mapsto subject} - Cert)$$

where
$CAT \in (ID, AT)$
$issuer \in (HCA_i, HTA_j)$, $i \in (1, \cdots, p)$, $j \in (1, \cdots, q)$
$subject \in m_1$

then I will issue you an authorization certificate $AU_{m_2 \mapsto m_1} - Cert$.

- $CCA_{m_1} - agent$: Hello, $SCA_{m_2} - agent$. Here are your required certificates in CNF. Please verify them and grant me an authorization certificate $AU_{m_2 \mapsto m_1}$ so that I can have resource access authority RS_i for my own delegatee agents.
- $SCA_{m_2} - agent$: Verification proceeds $\cdots$ and everything is OK. Hi, $CCA_{m_1} - agent$, here is $AU_{m_2 \mapsto m_1} - Cert$ (attached with Id_{m_2}'s signature).
- $CCA_{m_1} - agent$: Thank you, $SCA_{m_2} - agent$. I can proceed with my own multi-agent authority delegation now.

6.2.2. *Agent Certificate Showing, Delegation, and Verification Protocols*

1. Initial agent certificate issuing and storing

   Assuming that agent identity certificates are issued and stored in a specific agent platform.

2. Agent o_1 obtains an initial $AU_{m_1 \mapsto o_1} - Cert$ from $AU_{m_1} - agent$ embedded in $CCA_{m_1} - agent$.

3. Agent authority delegation network protocols in the agent cyberspace.

   - $AU_{m_1} - agent$: Hi agent o_1, here is $AU_{m_1 \mapsto o_1} - Cert$. Please use it to perform mediation services [6] for me to achieve the goal G.

[6] Agents o_1, o_2, o_3, and o_4 only provide pure mediation services and the willingness to provide their services is indicated in the services registration process whereas $RU_{m_2} - agent$ is a real resource access control agent to grant the final tangible or intangible resources.

- Agent o_1 (use multicast to send this $AU-Cert$ to agent $o_i, i \in (2,3,4)$ separately) : Hi agent o_i, where $i \in (2,3,4)$, $AU_{o_1 \mapsto threshold((j)o_i, j=2, i \in (2,3,4))} - Cert$ is the authorization certificate. Based on this certificate, please use threshold delegation mechanism to coordinate with agent $o_i, i \in (2,3,4)$. Make sure that at least j agents agree to perform the further authority delegation.

  (Assuming that agent o_2 initiates the coordination process and uses the threshold-initiate conversation act to obtain an authorization certificate from agent o_3.)
- Agent o_2: Hi agent o_3, I use the threshold-initiate conversation act to request that you send me your re-delegation threshold authorization certificate that was from agent o_1, i.e., $AU_{o_1 \mapsto threshold((j)o_i, j=2, i \in (2,3,4))} - Cert$ so that I can proceed with my chain-ruled delegation in the delegation network.
- Agent o_3: Hi agent o_2. Here is $AU_{o_3 \mapsto threshold_{o_2}} - Cert$. Hope everything is OK.
- Agent o_2: Thank you agent o_3 for your threshold re-delegation authority.

In order to achieve the Goal G, a series of delegation mechanisms including chain-ruled, threshold, and conditional delegations, etc, are applied in the delegation network from agent o_2 to the other mediation service agents. Agent r is the actual final resources request agent.

4. $AU-Cert$s verification process in the PAE by the $RU_{m_2} - agent$ embedded in the $SCA_{m_2} - agent$.

   - Agent r: Hi $RU_{m_2} - agent$. Here are my collective $AU_{(s_1, \cdots, s_n) \mapsto r} - Cert$s from my previous delegator agent $\in (s_1, \cdots, s_n)$. Hope you verify them and unlock your resource access authority RS_i.
   - RU_{m_2}-agent: Hi agent r. Based on my delegation logic rules and facts in the PAE, the verification process is proceeding, $\cdots$. Verification is complete and your request for resource access authority RS_i is granted.
   - Agent r: Thank you.

The human and agent certificate showing, delegation, and verification protocols were shown above as human understandable sentences. In

our further study, these human-based conversation protocols will be implemented in agent communication language with associated semantic web ontologies to fulfill the autonomous agent conversation protocols that are compliant with the future FIPA agent security standards (FIPA01b, 2001b) (Hendler, 2001).

7. AMEC Transactions Models

Under our agent-oriented PKI framework, we will show how a trusted AMEC transaction service is achieved via digital certificate management. The AMEC transaction models that we consider in this paper are C2B, C2C, B2B, and P2P.

7.1. C2B MODEL

The C2B transaction model is one of the most popular e-commerce services on the Internet. Even the secure socket layer (SSL) already provides a basic secure communication between the browser and web server. Certificate-based access control provides more robust and secure trusted transaction services than SSL (see *Figure 4*).

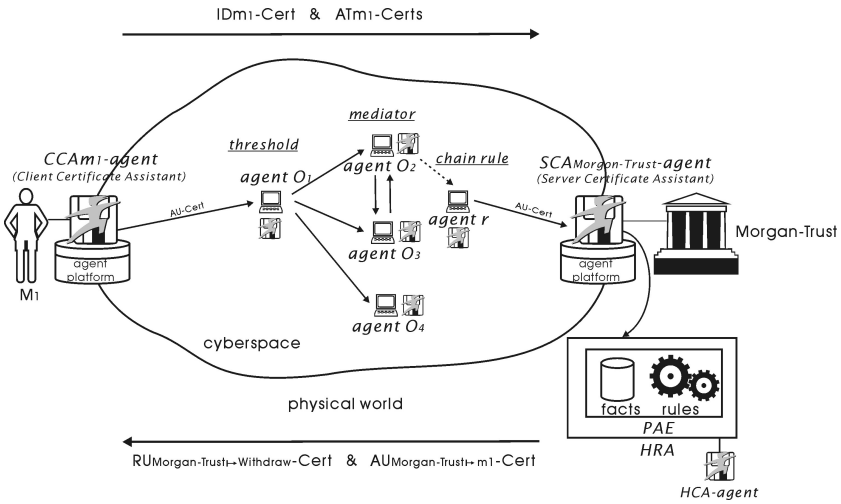

Figure 4. The trust establishment infrastructure for the C2B AMEC transaction services

7.1.1. *Closed group delegation*
Internet bank Morgan-Trust provides customer m_1 with valid $ID-Cert$ and bank account's $AT-Cert$ to perform a variety of transaction operations, such as check, withdraw, transfer, and deposit, on his account on the Internet. In this delegation scenario, all of the $AT-Cert$ issuers are the same as the resource owners so the attribute certificate verification process is a closed loop with respect to the $RU_{Morgan-Trust} - agent$.

The rules and facts for human certificate showing and verification protocols are shown in the following:

Rules

1. Morgan-Trust delegates the *issuing* operations for $ID_{HCA \mapsto h} - Cert = (?Id_h, ?Pu_h, ?V, Option, ?Sig_{HCA})$ to HCA If $HCA \in (E - Trust)$.

2. Morgan-Trust delegates the *issuing* operations for $AT_{HTA \mapsto h} - Cert = (?Id_h, ?IsAccountOwner(?Id_h, ?Acc), ?V, Option, ?Sig_{HTA})$ to HTA If $HTA \in (Morgan - Trust)$.

3. Morgan-Trust delegates the operations for $(Check(?Id_h, ?Acc), Withdrawal(?Id_h, ?Acc, ?Val), TransferFrom(?Id_h, ?Acc, ?Val), Deposit(?Id_h, ?Acc, ?Val))$ to $Name(?Id_h)$ If $ID_{HCA \mapsto h} - Cert \wedge AT_{HTA \mapsto h} - Cert \wedge IsAccountOwner(?Id_h, ?Acc) \wedge IsAccountBalance(?Val \geq 0, ?Acc)$.

4. Morgan-Trust says $PublicKey(?Pu_h)$ speaks for $Name(?Id_h)$ with role as $IsAccountOwner(?Id_h, ?Acc)$ on the operations for $(Check(?Id_h, ?Acc), TransferFrom(?Id_h, ?Acc, ?Val), Withdrawal(?Id_h, ?Acc, ?Val), Deposit(?Id_h, ?Acc, ?Val))$ If $IsPublicKey(?Pu_h, ?Id_h)$.

Facts

- $ID_{E-Trust \mapsto m_1} - Cert = (Id_{m_1}, 12345, 2001/01/01 - 2002/12/31, Option, Sig_{E-Trust})$
- $AT_{Morgan-Trust \mapsto m_1} - Cert = (Id_{m_1}, IsAccountOwner(Id_{m_1}, B10234), 2001/02/02 - 2002/12/31, Option, Sig_{Morgan-Trust})$
- IsPublicKey(12345,Id_{m1})
- IsPublicKey(45123,Id_{o_1})
- IsPublicKey(51234,Id_r)

– IsPublicKey(23456,$Id_{E-Trust}$)

– IsPublicKey(34567,$Id_{Morgan-Trust}$)

– IsAccountOwner(Id_{m_1},B10234)

– IsAccountBalance($5000,B10234)

`Human Certificate Showing, Delegation, and Verification Protocols`

– $CCA_{m_1} - agent$: I am m_1's personal agent (see my attached $ID_{E-Trust \mapsto m_1} - Cert$). May I have $Withdrawal(12345, B10234,$ $3000) access authority?

– $SCA_{Morgan-Trust} - agent$: Hi $CCA_{m_1} - agent$, you need to have the attribute certificate indicated in the following rule certificate:

$RU_{Morgan-Trust \mapsto Withdrawal(\cdots)} - Cert = (Withdrawal(\cdots),$ $AT_{Morgan-Trust \mapsto m_1} - Cert,\ Sig_{Morgan-Trust})$.

– $CCA_{m_1} - agent$: Here is your requested attribute certificate $AT_{Morgan-Trust \mapsto m_1} - Cert$.

– $SCA_{Morgan-Trust} - agent$: I am going to verify your $AT_{Morgan-Trust \mapsto m_1} - Cert$ validity and store the associated information as facts. Certificate verification and inference proceeding $\cdots$. A human-based authorization certificate is created as:

$AU_{Morgan-Trust \mapsto m_1} - Cert =$
$(34567, 12345, Withdrawal(12345, B10234, \$5000), 1,$
$2002/02/02 - 2002/02/06, SIG_{Morgan-Trust})$

Rules were explicitly shown in the Lampson's delegation logic using $SCA_{Morgan-Trust} - agent$ to declare the issuing requirements for an initial authorization certificate for $CCA_{m_1} - agent$. For example, rules 2 and 3 indicate the precondition for issuing an $AU_{Morgan-Trust \mapsto m_1} - Cert$. The facts are dynamically stored as long as the identity and attribute certificates or updated information are verified successfully. Therefore thee authorization certificate for $withdrawal(\cdots)$ in the rule head will not be fired unless all of the rule body CNF are resolved with the recently verified facts.

The delegation bit D is 1 in $AU_{Morgan-Trust \mapsto m_1} - Cert$ and this implies that further chain-ruled delegation is allowed for $AU_{m_1} - agent$. So once $CCA_{m_1} - agent$ has the $AU_{Morgan-Trust \mapsto m_1} - Cert$, it might re-delegate this withdrawal access authority to other mediator agents for mediation services, as shown in section 6.2.2.

– chain-ruled and conditional delegation

  Agent $AU_{m_1} - agent$ delegates the operations for *(check, withdrawal)* to agent o_1 on Internet bank *Morgan* with account $B10234$ under the conditions that the amount of $withdrawal(45123, B10234, \$1000)$ in one day from 2002/02/02 to 2002/02/06.

– threshold delegation

  Agent o_1 says threshold $(2, [o_2, o_3, o_4])$ speak for agent o_1 on the operations for *(check(45123,B10234), $withdrawal(45123, B10234, \$1000)$)* on the Internet bank *Morgan* in one day from 2002/02/02 to 2002/02/03.

On the final withdrawal permission request, agent r submits $withdrawal(51234, B10234, \$1000)$ authorization certificates to $RU_{Morgan-Trust} - agent$ for withdrawal permission (shown as below):

$$AU_{(s_1,\cdots,s_n)\mapsto r} - Certs = (*, 51234, Withdrawal(51234, B10234, \$1000),$$
$$0, 2002/02/02 - 2002/02/02, SIG_{(s_1,\cdots,s_n)})$$

The above authorization certificates are collected by agent r from the previous authority delegators using chain-ruled, threshold, and conditional delegation mechanisms. Of course these authorization certificates are possibly collected by $RU_{Morgan-Trust} - agent$ or other TTPs to provide more efficient certificate management and verification.

Finally the $RU_{Morgan-Trust} - agent$ initiates the PAE's inference rules and facts with these $AU_{(s_1,\cdots,s_n)\mapsto r} - Cert$s and the original $AU_{Morgan-Trust\mapsto m_1} - Cert$ decides whether the withdrawal permission request can be granted.

7.1.2. *Open group delegation*

Instead the attribute certificate issuer must be $AT_p - agent$ in $SCA_p - agent$ of the resource provider. Open group delegation allows $AT - Cert$s issuers to be other well-known TTPs declared by the $RU_p - agent$. The certificates verification process is therefore an open loop with respect to the $RU_p - agent$.

A researcher m_1 is going to apply for financial support from the NSF (National Science Foundation)-Trust to participate in the AMEC 2002 conference. The NSF-Trust requirements for the approval of financial support must have the following digital certificates: (1) an

applicant must have a legal citizenship (2) an applicant must be an faculty member at an MOE(Minister of Education) certified university (3) an applicant must have full paper(s) accepted by the AMEC 2002 conference. It is quite obvious that (1) is the identity certificate and (2), (3) are the attribute certificates. All of the above three digital certificates were not issued and endorsed by NSF-Trust so this is an open group delegation.

Rules

1. NSF-Trust delegates the *issuing* operations for $ID_{HCA \mapsto h} - Cert = (?Id_h, ?Pu_h, \overline{?V, Option}, ?Sig_{HCA})$ to HCA If $HCA \in (US{-}Trust)$.

2. NSF-Trust delegates the *issuing* operations for $AT_{HTA \mapsto h} - Cert_1 = (?Id_h, ?\overline{IsFacultyOf}(?Id_h, ?Id_{HTA}), ?V, Option, ?Sig_{HTA})$ to HTA
   If HTA *has* $AT_{MOE-Trust \mapsto HTA} - Cert_2$.

3. NSF-Trust delegates the *issuing* operations for $AT_{HTA \mapsto h} - Cert_3 = (?Id_h, ?\overline{IsFullPaperAcceptedBy}(?Id_h, ?Id_{HTA}), ?V, Option, ?Sig_{HTA})$ to HTA
   If $HTA \in (ACM - Trust, IEEE - Trust, AMEC - Trust, \cdots)$.

4. NSF-Trust delegates the operation for $(UseTravelCredit(?Id_h, ?T - Amount) \wedge UseRegistCredit(?Id_h, ?R - Amount))$ to $Name(?Id_h)$
   If $ID_{HCA \mapsto h} - Cert \wedge AT_{HTA \mapsto h} - Cert_1 \wedge AT_{HTA \mapsto h} - Cert_3$.

5. NSF-Trust says $PublicKey(?Pu_h)$ speaks for $Name(?Id_h)$ with role as $\overline{IstheAuthorFor}(?Id_h, ?Id_{HTA})$ on the operations for $(UseTravelCredit(?Id_h, ?T - Amount) \wedge UseRegistCredit(?Id_h, ?R - Amount))$
   If $IsPublicKey(?Pu_h, ?Id_h)$.

Facts

- $ID_{US-Trust \mapsto m_1} - Cert = (Id_{m_1}, 12345, 2001/01/01 - 2002/12/31, Option, Sig_{US-Trust})$
- $AT_{NCCU-Trust \mapsto m_1} - Cert_1 = (Id_{m_1}, IsFacultyOf(Id_{m_1}, Id_{NCCU-Trust}), 2001/02/02 - 2004/12/31, Option, Sig_{NCCU-Trust})$
- $AT_{MOE-Trust \mapsto NCCU-Trust} - Cert_2 = (Id_{NCCU-Trust}, IsCertifiedBy(Id_{NCCU-Trust}, Id_{MOE-Trust}), 2001/02/02-, Option, Sig_{MOE-Trust})$

- $AT_{AMEC-Trust \mapsto m_1} - Cert_3 = (Id_{m_1}$, $IsFullPaperAcceptedBy(Id_{m_1}, Id_{AMEC-Trust})$, $2002/02/02 - 2002/02/31, Option, Sig_{AMEC-Trust})$
- IsPublicKey(12345,Id_{m1})
- IsPublicKey(54321,$Id_{NSF-Trust}$)
- IsPublicKey(56789,$Id_{NCCU-Trust}$)
- IsPublicKey(67891,$Id_{MOE-Trust}$)
- IsPublicKey(78912,$Id_{AMEC-Trust}$)

`Human Certificate Showing, Delegation, and Verification Protocols`

- $CCA_{m_1} - agent$: I am m_1 personal agent (see my attached $ID_{US-Trust \mapsto m_1} - Cert$). May I have $UseTravelCredit(\cdots) \wedge UseRegistCredit(\cdots)$ access authorities to present my acceptance paper at the $AMEC$ 2002 conference?
- $SCA_{NSF-Trust} - agent$: Hi $CCA_{m_1} - agent$, you need to satisfy the following rule certificate with the corresponding attribute certificates:

  $RU_{NSF-Trust \mapsto UseTravelCredit(\cdots) \wedge UseRegistCredit(\cdots)} - Cert =$ $(UseTravelCredit(\cdots) \wedge UseRegistCredit(\cdots)$, $AT_{HTA \mapsto m_1} - Cert_1$, where HTA has $AT_{MOE-Trust \mapsto HTA} - Cert_2$ $\wedge$ $AT_{AMEC-Trust \mapsto m_1} - Cert_3$, where $HTA \in (ACM - Trust$, $AMEC - Trust, \cdots)$, $Sig_{NSF-Trust})$.

- $CCA_{m_1} - agent$: Here are your requested attributed certificates:

  $AT_{NCCU-Trust \mapsto m_1} - Cert_1 \wedge AT_{AMEC-Trust \mapsto m_1} - Cert_3$

- $SCA_{NSF-Trust} - agent$: Facts store and verification proceeds$\cdots$. Verification is complete and success [7], and an $AU - Cert$ will be issued for you as follows:

  $AU_{NSF-Trust \mapsto m_1} - Cert = (54321, 12345,$ $UseTravelCredit(12345, \$3000) \wedge UseRegistCredit(12345, \$1000)$ $, 1, 2001/02/02 - 2002/12/31, Sig_{NSF-Trust})$

[7] Here, $SCA_{NSF-Trust} - agent$ must verify $AT_{MOE-Trust \mapsto NCCU-Trust} - Cert_2$ before $AT_{NCCU-Trust \mapsto m_1} - Cert_1$ is verified successfully.

Agent Certificate Showing, Delegation, and Verification Protocols

Once the $CCA_{m_1} - agent$ has the authorization certificate, it might use $UseTravelCredit(12345, \$3000)$ authority to delegate the mediation service to the travel agent and use $UseRegistCredit(12345, \$1000)$ authority to delegate the mediation service to the registration agent. The entire chain-ruled, conditional, and threshold delegation processes are quite similar to the closed group delegation scenario.

7.2. C2C MODEL

The C2C AMEC model can be implemented as pure closed group delegation where all of the trader attribute certificates must be issued by the trading center. We would rather model C2C as an open group delegation because it is not always true that all of the trader attribute certificates are issued by the trading center (see *Figure 5*).

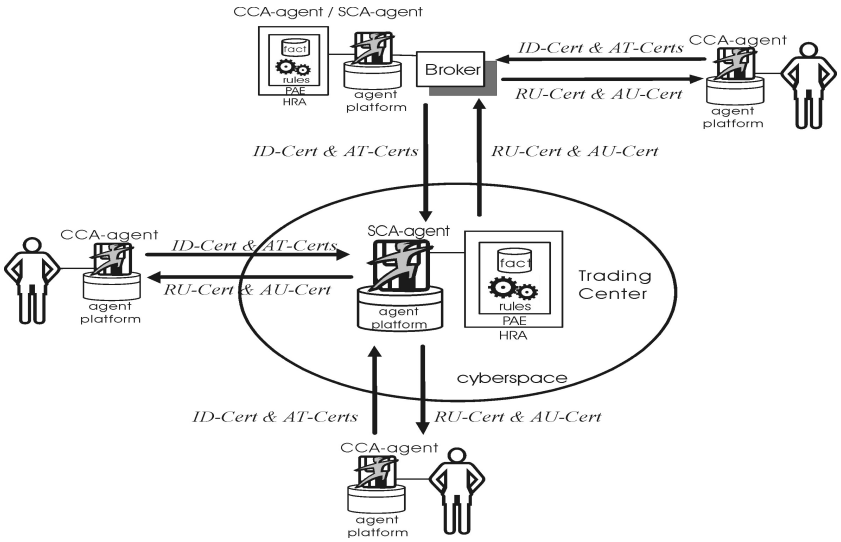

Figure 5. The trust establishment infrastructure for the C2C AMEC transaction services

For example, the NYSE is one of the well-known stock trading centers for stock traders to buy and sell stocks. We might delegate Morgan-Trust Internet bank or other Internet e-commerce traders as our stock trading broker to buy and sell stocks in the NYSE. The attribute certificates that provide initial delegation authority are issued by stock brokers instead of NYSE-Trust.

These stock broker institutions certainly have attribute certificates declared by NYSE-Trust. They therefore have legal authority to provide

stock trading mediation services. Of course, stock buyers and sellers can trade directly in the NYSE trading center via Internet access but they still must prepare certain attribute certificates to satisfy the trading policies declared by NYSE-Trust.

Rules declared and facts stored in *HRA* are very similar to the previous C2B model. We are therefore not going to show them explicitly. In the C2C AMEC model, an auction server usually provides a trust infrastructure to enforce the rules for all sellers and buyers whereas in the C2B AMEC model the customers and merchants enforce the trust mechanisms for their own control purposes.

7.3. B2B MODEL

This will be one the most promising AMEC studies in B2B agent-based business process management. Building a trusted AMEC infrastructure for B2B model will have significant influence on popularizing agent-oriented technology. The trust relationship of the C2B model is based on loosely market-oriented transaction services, whereas the trust establishment of B2B transaction services is usually based on institution vs. institution longstanding relationships (Dignum, 2001).

Agents are therefore the delegatee of electronic institutions instead of human beings in the B2B model. Building an agent-oriented PKI for B2B model involves enforcing the trust and authority delegation within the electronic institution as well as among electronic institutions (see *Figure 6*).

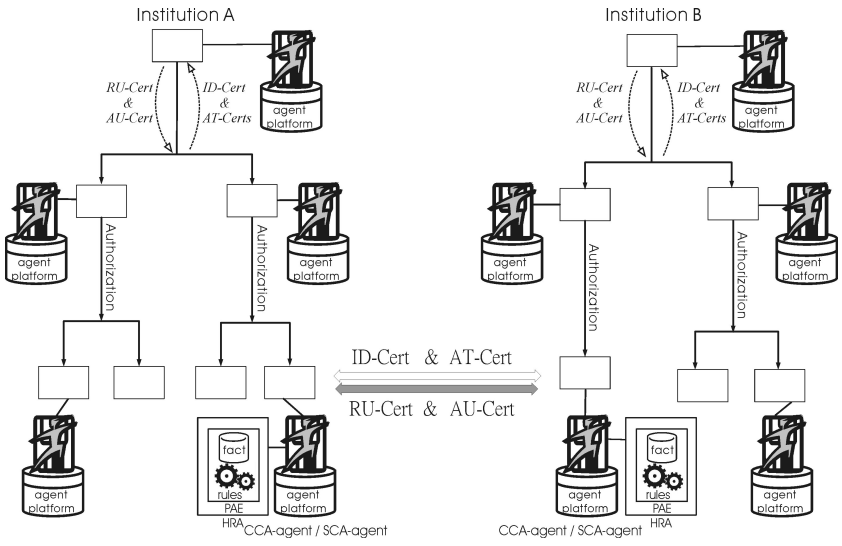

Figure 6. The trust establishment infrastructure for the B2B AMEC transaction services

In the B2B model, the trust establishment is also based on human and agent certificate showing, delegation, and verification protocols that were shown in section 6.2. Facts and rules for each department and institution can be stored and declared as in the C2B model, so we are not going to reiterate the process here.

– Trust within an electronic institution

  An agent is enacted as a department's delegatee within the electronic institution so the trust issue in this scenario involves ensuring that delegation mechanisms among department agents are verifiable. As an agent is the delegatee of each department, after using possible delegation mechanisms, such as chain-ruled, threshold, and conditional delegations, the entire electronic institution is able to authorize a legal agent to act as the institution delegatee. The design and verification of an authorization certificate can be simplified if we can use role-based authentication/authorization access control (Herzberg et al., 2000)

– Trust among electronic institutions

  The trust issue among electronic institutions involves verifying the validity of authorization certificates presented by the peer side's legal delegatee agent. The authorization certificates are based on the authorization tree that was issued and signed by a legal enable agent within the electronic institution to declare its resource request intentions (Ludwig et al., 2000). In the B2B transaction service, the resource provider agent verifies these authorization certificates to guarantee that all of the agent-oriented transaction services are trusted, legal and non-repudiated.

7.4. P2P MODEL

In a P2P e-commerce model, information and resource sharing are based on a fully distributed service environment. Potential applications for P2P services involve content-based information sharing and computing resource power sharing, etc. We proposed an ad hoc authentication and authorization control mechanism to remedy the existing lack of trust and secure infrastructure for P2P transaction services (Lee and Hu, 2001). In P2P transaction services, the boundary for resource consumers and providers is pretty vague, i.e., any principal can play both consumer and provider to ensure that all of the information and services can be widely distributed on the Internet (see *Figure 7*).

We propose that any agent who is going to export its information and resources for sharing with the other agents provide a trusted AMEC

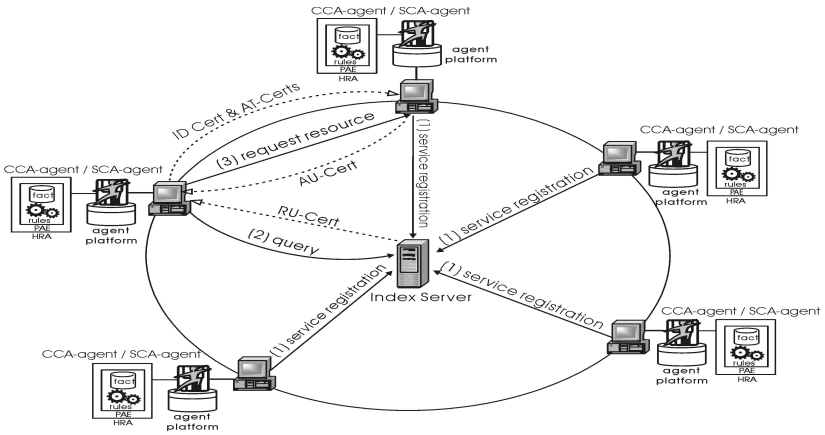

Figure 7. The trust establishment infrastructure for the P2P AMEC transaction services in the centralized index server scenario. In this model each peer agent is embedded with both $CCA_p - agent$ and $SCA_p - agent$ service capabilities.

service for P2P model during the service registration process. This agent must then declare its sharing rule policies and store these policies either in the centralized or in the distributed index server.

In the centralized index server scenario, the information or resource consumer agent queries the index server to visualize what the digital certificate requirements are for a particular information category. The trust establishment process between information consumer agent and provider agent will then be executed as in the C2B model.

In the distributed index server scenario, the trust establishment handshaking protocols for any two peer sides are initiated by the information consumer agent to request the authorization certificate from the information provider agent once a service match is found (Lee and Hu, 2001). This approach is thus an ad hoc trust establishment between peer agents when compared with the centralized index server scenario.

8. Trusted AMEC System Implementation

We are implementing an agent-oriented PKI to verify our agent certificate theory on trusted AMEC systems in the FIPA-OS (Open Source) agent platform [8]. Because of the lack of trust and security mechanisms in the FIPA architecture, we use only the **Request/Agree** protocol to declare identity and authorization certificates in the agent communication language (ACL) (FIPA01b, 2001b). These authorization

[8] see http://FIPA-os.sourceforge.net

certificates might be collected by delegatee agents or resource control agents in the chain-ruled delegation process to ensure authority granting trust in the entire delegation path.

We envision the requirements for the new communicative acts for the management of agent digital certificates (Hu, 2001). Otherwise there is a big overhead for agents to parse deep recursive ACL message when getting associated digital certificates. These new performatives for agent certificate management are easily embedded in the XML DTD file in fipa.acl.rep.xml.std (FIPA01c, 2001c). At this moment our certificate management framework is a plug in module instead of a built-in module for FIPA-OS. This approach can be improved when the FIPA consortium accepts our proposal for new communicative acts for agent communication.

9. Further Studies

We are constructing an agent-oriented PKI system to evaluate and verify our certificate-based trust establishment problem. This is an ongoing implementation process for the generic secure multi-agent system framework. We found that this research direction is quite promising when a similar trust semantic web issue was also presented by Tim Berners-Lee at the XML 2000 conference. In our further studies, we are considering using our certificate-based trust establishment theory for agent-based e-services in the semantic web environment. This is the most trivial shortcoming for the semantic web services, such as DAML-S (Ankolekar et al., 2001) (Mcllraith et al., 2001).

RuleML is an emerging rule markup language for semantic web rules (Boley et al., 2001)(Grosof and Labrou, 1999). We are also planning to encode our trust verification rules in Rule Markup (RuleML) to ensure inference rules portability and interoperability.

10. Conclusion

There are several emerging issues and challenges in AMEC studies. Among them, we envision the importance of building an AMEC environment with verifiable trust establishment among agents. In this study, we proposed a certificate theory to verify agent trust with respect to authentication, authorization, and delegation control criteria. An agent-oriented PKI framework was constructed to achieve these objectives. Human and agent certificates showing, delegation, and verification protocols were specified using this infrastructure to show our trust establishment methodology.

The feasibility of these verification protocols was demonstrated for several well-known AMEC transaction services models. We implemented trusted multi-agent systems on an FIPA compliant standard agent platform to validate our certificate theory.

References

Abadi, M., M. Burrows, and B. Lampson. (1993). "A Calculus for Access Control in Distributed Systems." *ACM Transactions on Programming Languages and Systems,* 15(4), pp. 706-734.

Ankolekar, A., et al.. (2001). " DAML-S: Semantic Markup For Web Services." *Proceedings of the First Semantic Web Working Symposium, SWWS'01,* Stanford University, California, USA, Jul 30 - August 1, pp. 411-430.

Aura, T. (1999). "Distributed Access-Rights Management with Delegation Certificates." *Secure Internet Programming: Security Issues for Mobile and Distributed Objects,* LNCS 1603, Springer-Verlag, pp. 213-238.

Bailey, P. J. and Y. Bakos. (1997). "An Exploratory Study of the Emerging Role of Electronic Intermediaries." *International Journal of Electronic Commerce,* Vol. 1, No. 3, pp. 7-20.

Blaze, M., J. Feigenbaum, J. Ioannidis, and A. D. Keromytis. (1999). "The Role of Trust Management in Distributed System Security." *Secure Internet Programming: Security Issues for Mobile and Distributed Objects,* LNCS 1603, Springer-Verlag, pp. 185-212.

Boley, H., S. Tabet, and G. Wagner. (2001). "Design Rationale of RuleML: A Markup Language for Semantic Web Rules." *Proceedings of the First Semantic Web Conference,* Stanford, CA, pp. 381-402.

Castelfranchi, C. and R. Falcone. (2000). "Trust and Control: A Dialectic Link." *Applied Artificial Intelligence,* 14, pp. 799-823.

Dignum, F. (2001). "Agents, markets, institutions and protocols." *Agent Mediated Electronic Commerce: The European AgentLink Perspective*, Springer, pp. 98-114.

Ellison, C. M. (2001). "SPKI/SDSI Certificates." `http://world.std.com/`

Farrell, S. and R. Housley. (2001). "An Internet Attribute Certificate Profile for Authorization." draft-ietf-pkix-ac509prof-06.txt. `http://www.ietf.org`.

FIPA01a. (2001a). FIPA Agent Management Specification. document no. XC00023 `http://www.fipa.org`.

FIPA01b. (2001b). FIPA Communicative Act Library Specification. document no. XC00037. `http://www.fipa.org`.

FIPA01c. (2001c). FIPA ACL Message Representation in XML Specification. document no. XC00071. `http://www.fipa.org`.

Gerck, E. (2000). "Overview of Certification Systems: X.509, CA, PGP and SKIP.", MCG-Meta-Certificate Group, `http://www.mcg.org.br`.

Grosof, N. B. and Y. Labrou. (1999). "An Approach to using XML and a Rule-based Content Language with an Agent Communication Language." *IBM Research Report,* RC 21491(96965), `http://www.research.ibm.com`.

He, Q., K. Sycara, and T. Finin. (1998). "Personal Security Agent: KQML-Based PKI." *Proceedings of the Second International Conference on Autonomous Agents.*

Heckman, C. and O. J. Wobbrock. (2000). "Put Your Best Fact Forward: Anthropomorphic Agents, E-Commerce Consumers, and the Law." *Proceedings of the Fourth International Conference on Autonomous Agents*, Barcelona, pp. 435-441.

Hendler, J. (2001). "Agents and the Semantic Web." *IEEE Intelligent System,* Vol. 16, No. 2, March-April, pp. 30-37.

Herzberg, A. et al. (2000). "Access Control Meets Public Key Infrastructure, Or: Assigning Roles to Strangers." *2000 IEEE Symposium on Security and Privacy,* pp. 2-14.

Hu, Y. J. (2001). "Some Thoughts on Agent Trust and Delegation." *Proceedings of the Fifth International Conference on Autonomous Agents,* May 28-June 1, Montreal, Quebec, Canada, pp. 489-496.

Jennings, R. N., K. Sycara, and M. Wooldridge. (1998). "A Roadmap of Agent Research and Development." *Autonomous Agents and Multi-Agent Systems,* 1, pp. 7-38.

Johnston, W., S. Mudumbai, and M. Thompson. (1998) "Authorization and Attribute Certificates for Widely Distributed Access Control." *Proceedings of the IEEE 7th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises - WETICE'98.*

Kohnfelder, L. M. (1978). *Towards a Practical Public-key Cryptosystem*, MIT S. B. Thesis, May.

Kohlas, R. and Maurer. (1999). "Reasoning About Public-Key Certification: On Binding Between Entities and Public Keys." *Financial Cryptography 99 (FC99),* Lecture Notes of Computer Science, Springer-Verlag.

Lampson, B., M. Abadi, M. Burrows, and E. Wobber. (1992). "Authentication in Distributed Systems: Theory and Practice." *ACM Trans. Computer Systems,* 10, 4, Nov., pp. 265-310.

Lee, Ing-Chung and Y. J. Hu. (2001). "An Agent-Based Secure E-Commerce Environment with Distributed Authentication and Authorization Services." *The 2001 International Conference on Internet Computing(IC-2001) Session on Agents for E-Business on the Internet,* Monte Carlo Resort, Las-Vegas, USA, June 25-28.

Li, N., B. N. Grosof, and J. Feigenbaum. (1999). "A Logic-based Knowledge Representation for Authorization with Delegation." *IBM Research Report,* RC 21492(96966), May. texttthttp://www.research.ibm.com.

Ludwig, H., L. O'Connor, and S. Kramer. (2000). "Method for Inter-Enterprise Role-Based Authorization." *First International Conference, EC-Web 2000,* London, UK, pp. 133-144.

Mcllraith, A. Sheila, Tran Cao Son, and Honglei Zeng. (2001). "Mobilizing the Semantic Web with DAML-Enabled Web Services." *Proceedings of the Second International Workshop on the Semantic Web-SemWeb'2001,* Hong Kong, China, May 1, 2001, pp. 82-87.

Moukas, A., R. Guttman, G. Zacharia, and P. Maes. (2000). "Agent-mediated Electronic Commerce: An MIT Media Laboratory Perspective." *International Journal of Electronic Commerce,* Vol. 4, No. 3.

Nwana, S. H., et al. (1998). "Agent-Mediated Electronic Commerce: Issues, Challenges and Some Viewpoints." *Proceedings of the Second International Conference on Autonomous Agents*, pp. 189-196.

Park, S. J. and R. Sandhu. (2000). "Binding Identities and Attributes Using Digitally Signed Certificates." *16th Annual Computer Security Applications Conference (ACSAC)*, New Orleans, Louisiana, Dec.

Sarkar, M. B., B. Bulter, and C. Steinfield. (1995). "Intermediaries and Cybermediaries: A Continuing Role for Mediating Players in the Electronic Marketplace." *Journal of Computer-Mediated Communication,* Vol. 1, No. 3. `http://jcmc.huji.ac.il/vol1/issue3/sarkar.html.`

Sierra, C. (1999). *Agent-mediated Electronic Commerce: Scientific and Technology roadmap.* `http://www.iiia.csic.es/AMEC/.`

Vulkan, N. (1999). "Economic Implications of Agent Technology and E-Commerce." *The Economic Journal,* 109 February, pp. 67-90.

Winslett, M., N. Ching, V. Jones., and I. Slepchin. (1997). "Using Digital Credentials on the World-Wide Web." *Journal of Computer Security.* `http://drl.cs.uiuc.edu/security/pubs.html.`

Winsborough, H. S. William, E. Kent, and V. E. Jones. (1999). "Negotiating Disclosure of Sensitive Credentials." *Second Conference on Security in Communication Networks,* Amalfi, Italy.

Wong, H. C., and K. Sycara. (1999). "Adding Security and Trust to Multi-Agent Systems." *Proceedings of Third International Conference on Autonomous Agents (Workshop on Deception, Fraud and Trust in Agent Societies)*, May, Seattle, Washington, pp. 149-161.

Zacharia, Giorgos and P. Maes. (2000). "Trust Management Through Reputation Mechanisms." *Applied Artificial Intelligence,* 14, pp. 881-907.